APPENDIX E

HAZARD ANALYSIS GUIDELINES

These guidelines are intended to help the test developer define "hazard analysis," identify hazards in the test equipment and procedures, and prepare the hazard analysis required for the test equipment data package described in Section 6.4.3 of this document.

1. EXPERIMENT HAZARD EVALUATION

   This portion of the data package should contain a brief summation of the results of an intensive review of the experiment hardware and planned test operations to identify potential hazard sources inherent in either the experiment equipment or test operations. In attempting to identify these hazards, the individual performing the evaluation should keep in mind "Murphy's Law" which states, "If anything can go wrong, it most likely will go wrong." During the evaluation process, the evaluator should take a "devil's advocate" position in the review of the experiment design, performance configuration, and planned operations. All hazards which could cause injury to flight test personnel or adversely affect the flight worthiness of the KC-135 aircraft should be carefully assessed in this process, no matter how remote the possibility of such an occurrence might seem. To aid in this process, a "Hazard Source Checklist" has been included as Enclosure 1 of this appendix.

   The evaluator should note that a potential hazard should not be ignored and left unidentified just because stringent precautions have been taken to prevent the hazard from occurring.

   Such precautions are called "Hazard Controls." The proper approach to such a situation is to identify both the hazard and the controls utilized to prevent its occurrence. Another common error in hazard identification frequently occurs when the evaluator determines that a condition or situation normally considered a hazard should not be included in the hazard evaluation because it is not considered to be a "credible" hazard. An example illustrating this point is the use in an experiment of a very small amount of a toxic substance such as mercury which, for photographic purposes, must be placed in a glass container. Because the quantity of mercury used is so small, the evaluator reasons that, even if the glass container breaks, there is no need to identify the mercury as a hazard source. This is not correct! The proper approach is to place the mercury on the hazard list and then demonstrate, by analytical means, that if all the available mercury were dispersed in the immediate environment, the maximum concentration possible would still be within acceptable industrial hygiene limits. Only after such an evaluation can the mercury be considered to constitute a "non-credible" hazard.

   In the summation, the evaluator should identify those hazard sources which are considered most critical from a safety standpoint and those which require special or unique controls to ensure that a hazardous condition or accident will not occur. If the evaluation indicates that no significant hazards exist in the experiment or in planned experiment operations, the evaluator should so state.

2. HAZARD LIST

Based on the evaluation discussed in Section 1, the experimenter shall prepare a Hazard List which lists all potential hazards identified during the evaluation. Each hazard should be roughly categorized under the following "Generic Hazard" listings:

A. Radiation (ionizing, electromagnetic, laser)

B. Toxic Materials/Contamination

C. Explosion/Implosion

D. Fire

E. Collision/Impact

F. Loss of Habitable Environment

G. Electrical Shock/Static Discharge

H. Injury and/or Illness

I. Temperature Extremes

J. Structural Failure

K. Corrosion

L. Any others which may not fall into any of the above categories.

It should be noted that there is some overlap in the above hazard categories and, in some cases, it may not be readily obvious as to which category is most applicable to a particular hazard. The categorization of the hazards is not, in itself, critical, and, where the correct category is unclear, the analyst should use his or her best judgment.

In addition to grouping the hazards into categories, each hazard should be identified by a descriptive, but concise, hazard title which includes the hazard category (e.g., "Fire Resulting From LO_2 Leakage," "Toxic Material Release Into Cabin," etc.).

3. HAZARD REPORT PREPARATION

The experimenter must prepare a "Hazard Report" for each of the hazards identified in the above Hazard List. The format used for the Hazard Report is left to the discretion of the experimenter. However, it may be convenient to use a format similar or identical to the one shown in Enclosure 2 of this document. It should be noted that, whatever format is used, the report must contain those topics identified in Enclosure 2, including supporting data.

The basic purpose of a Hazard Report is to document the safety analysis performed to assure that all potential hazard causes have been addressed and adequate controls have been implemented. The report should be of sufficient depth and detail so that technical management personnel can determine if adequate hazard elimination or control has been accomplished or if additional hazard resolution analysis is required. The preparation of

Hazard Reports should begin during the conceptual phase of the experiment as hazards are identified and should continue throughout the experiment life cycle. Hazard Reports must be updated whenever changes to experiment design or operations affect the hazard condition addressed in the report.

Descriptions of the required contents of a Hazard Report follows:

A. Hazard Title--As stated in the last paragraph of Section 2 above, the title should be concise and descriptive, and should include the applicable hazard category (per Section 2).

B. Description of Hazard--This section should briefly describe the potential hazard in terms of the risk to flight test personnel and to the flight worthiness of the KC-135 aircraft structure and flight systems. The experimenter should take care to identify the actual hazard as opposed to the hazard cause. For example, the over-pressurization of a tank is a hazard cause, whereas the possible explosion of the tank (with the potential for catastrophic consequences) is the actual hazard. In the same vein, a pressure relief valve (PRV) attached to the tank would constitute a hazard control. A test showing that the valve actually opened at the required pressure would provide verification that the control was adequate.

C. Hazard Causes--This section of the hazard report should identify and itemize all potential events or factors which could create the specific hazard in question. The number of factors which could induce a specific hazard could conceivably vary from one to perhaps 10 or more. Again, it is very important that all possible causes be identified and analyzed. Referring to the example in Section 3.B above, the cause of the tank explosion could conceivably be any of the following factors:

    (1) Tank inadvertently under-designed for maximum operating pressure
    (2) One or more tank welds are defective
    (3) Tank not equipped with a PRV
    (4) The PRV failing to open at the correct pressure
    (5) Tank pressure gauge reading incorrectly
    (6) Tank failing because of error in operating procedure and/or software
    (7) Human error
    (8) Other possible factors not identified above.

    Each of the hazard causes identified above must be countered by one or more specific Hazard Controls. These controls are discussed in the following section.

D. Hazard Controls--Particular emphasis must be placed on thorough development of the contents of this section of the Hazard Report. Hazard control statements must be:

- Specific - Don't generalize.
- Complete - Identify all controls applicable to the specific hazard.

- Definitive - Provide adequate details to fully describe each control. This section must specifically identify the precise Hazard Control(s) utilized (such as redundancy or other design features, safety devices, warning devices, materials selection, and/or special operation procedures) that will eliminate, reduce, counter, or otherwise control the hazard(s) resulting from each Hazard Cause previously identified. Each Hazard Control must also be backed up by supporting data such as to "as-built" drawings, quality assurance inspection or certification procedures, schematics, materials lists, approved test procedures, etc. Referring again to the pressurized tank example of Sections 3.B and 3.C, examples of acceptable Hazard Control statements for two of the Hazard Causes listed in 3.C might be:

  (1) For Hazard Cause "a," a statement that "the pressure vessel has been designed to sustain maximum expected operating pressure with a safety factor of 4.0" would normally be acceptable.

  (2) For Hazard Cause "d," an appropriate statement might be "Redundant PRV's with proper relief pressure settings will be used on the pressurized tank." Specify relief pressure setting numbers (e.g., relief valve setting).

  If the experimenter determines that he has a potential hazard for which no suitable Hazard Control is available, the deficiency must be documented and brought forward as an uncontrolled hazard. This hazard will then be made visible to appropriate NASA management for a decision regarding risk acceptance.

E. Verification Method/Status--This portion of the Hazard Report should identify the verification method(s) to be used to demonstrate the effectiveness of each Hazard Control, the data/documentation/certification which will be provided to demonstrate that verification has been satisfactorily accomplished, and the status of each verification data item.

Basically, there are three verification methods which may be used by the experimenter in satisfying the verification requirements. These are:

(1) Test

(2) Inspection

(3) Analysis (both mathematical and data evaluation, such as review of design drawings, schematics, test results, etc.).

Test results will normally be documented by approved or certified test reports. Inspection results will be validated by such data as Quality Control Inspection Reports, Receiving Inspection Reports, Acceptance Reports, etc. Analytical results will be validated by such items as detailed structural stress analysis of the experiment, fracture mechanics analysis, thermal analyses, etc. Where applied to data such as design drawings, schematics, test results, etc., the term "analysis" should be interpreted as a detailed, critical review of the

drawing and test results to determine if they substantiate the claims made in the Hazard Control sections.

Referring to the example "Hazard Control" statements in Section 3.D, the "Verification Method/Status" statements for examples "a" and "b" might be worded as follows:

A. For Hazard Cause "a."

Verification Method/Status-Test & Analysis

(1) Test Procedure, TP-011-Complete. In Data Pack.

(2) Test Report, TR-011-Complete. In Data Pack.

(3) Fracture Mechanics Analysis-Complete. In Data Pack.

B. For Hazard Cause "b."

Verification Method/Status-Test & Analysis

(1) Acceptance Test Report, ATR-007-Complete. In Data Pack.

(2) Analysis of Plumbing Schematic, SC-P-001-Complete. In Data Pack.

4. Mandatory Verification Data for All Experiments

Certain verification documentation requirements are mandatory for all applicable experiments. These are:

1. A structural loads/stress analysis which demonstrates that the experiment can safely withstand the loads specified in Section 6.5.1 of this document.
2. A Pressure Vessel Certification document (if applicable) which meets the criteria specified in Section 6.5.2 of this document.
3. A Certificate of Compliance (if applicable), signed by the experimenter, stating that the experiment electrical system was designed and fabricated in accordance with Section 6.5.3 of this document.

HAZARD SOURCE CHECKLIST

_____ Flammable/combustible material, fluid (liquid, vapor, or gas)
_____ Toxic/noxious/corrosive/hot/cold material, fluid (liquid, vapor, or gas)
_____ High pressure system (static or dynamic)
_____ Evacuated container (implosion)
_____ Frangible material
_____ Stress corrosion susceptible material
_____ Inadequate structural design (e.g., low safety factor)
_____ High intensity light source (including laser)
_____ Ionizing/electromagnetic radiation
_____ Rotating device
_____ Extendible/deployable/articulating experiment element (collision)
_____ Stowage restraint failure
_____ Stored energy device (e.g., mechanical spring under compression)
_____ Vacuum vent failure (i.e., loss of pressure/atmosphere)
_____ Heat transfer (habitable area over-temperature)
_____ Over-temperature explosive rupture (including electrical battery)
_____ High/Low touch temperature
_____ Hardware cooling/heating loss (i.e., loss of thermal control)
_____ Pyrotechnic/explosive device
_____ Propulsion system (pressurized gas or liquid/solid propellant)
_____ High acoustic noise level
_____ Toxic off-gassing material
_____ Mercury/mercury compound
_____ Other JSC 11123, Section 3.8 hazardous material
_____ Organic/microbiological (pathogenic) contamination source
_____ Sharp corner/edge/protrusion/protuberance
_____ Flammable/combustible material, fluid ignition source (i.e., short circuit; under-sized wiring/fuse/circuit breaker)
_____ High voltage (electrical shock)
_____ High static electrical discharge producer
_____ Software error
_____ Carcinogenic material

Sheet 1 of _____

ENCLOSURE 1

EXPERIMENT/TEST EQUIPMENT HAZARD REPORT

PREPARER'S NAME: _____ HR NO: _____

PREPARER'S ORGANIZATION: _____

PHONE NUMBER: _____ DATE: _____

EQUIPMENT NAME: _____

_____

HAZARD TITLE: _____

_____

HAZARD DESCRIPTION: _____

_____

_____

_____

HAZARD EVALUATION:

1 EVALUATION OF CAUSE NO. 1

a. HAZARD CAUSE:

_____

_____

b. HAZARD CONTROL(S):

_____

_____

c. VERIFICATION METHOD(S)/STATUS:

_____

_____

ENCLOSURE 2

HR NO.: _____
Sheet 2 of _____

2. EVALUATION OF CAUSE NO. 2
   a. HAZARD CAUSE:

      _____

      _____

   b. HAZARD CONTROL(S):

      _____

      _____

   c. VERIFICATION METHOD(S)/STATUS:

      _____

      _____

3. EVALUATION OF CAUSE NO. 3

   (NOTE: Continue as above until all Hazard Causes applicable to the Hazard Title have been addressed. The experimenter should again note that a separate Hazard Report is required for each hazard identified in the Hazard List discussed in Section C of this appendix.)

ENCLOSURE 2
(continued)